

Защита данных с помощью шифрования диска BitLocker

BitLocker — мощное средство, разработанное для защиты от конкретных угроз, с чем оно прекрасно справляется. Но не стоит считать его панацеей. Совершенно необходимо продолжать использование остальных защитных и управляющих мер, например надежных паролей.

Шифрование дисков BitLocker — определенно одна из самых обсуждаемых возможностей в Windows Vista. Однако, большинство людей еще не имело серьезной возможности опробовать BitLocker и на собственном опыте испытать, что и как он делает — особенно на компьютере с доверенным платформенным модулем (TPM). В этой статье мы рассмотрим основы BitLocker™, позволяющие оценить его потенциал и включить в программу обновления. Начнем с предпосылок и концепций, затем рассмотрим включение BitLocker, восстановление данных, администрирование и то, какова роль BitLocker при утилизации компьютера.

BitLocker выполняет две взаимодополняющие, но различные функции. Во-первых, он обеспечивает шифрование всего тома ОС Windows®. Во-вторых, на компьютерах с совместимым доверенным платформенным модулем он позволяет проверить целостность загрузочных компонентов до запуска Windows Vista™.

Для полного использования возможностей BitLocker компьютер должен быть оснащен совместимыми микрочипом TPM и BIOS. Под совместимыми понимается версия 1.2 TPM и BIOS, поддерживающая TPM и статический корень измерения доверия (Static Root of Trust Measurement), определенный в спецификациях TCG. Однако компьютеры без совместимых TPM и BIOS тоже могут использовать шифрование BitLocker.

Полное шифрование тома

BitLocker шифрует весь том ОС Windows со всеми данными. Это ключевой аспект в защите конфиденциальной информации, содержащейся на компьютерах предприятия, особенно переносных.

Переносные компьютеры крадут и теряют каждый день. Благодаря возросшим возможностям переносных устройств, а также все большей доли мобильности в работе один сотрудник может иметь при себе сотни гигабайт промышленных секретов вашего предприятия, секретных документов или сведений о клиентах частного характера. Краткий обзор сводок новостей покажет, что такие данные теряются слишком часто. (По данным Privacy Rights Clearinghouse, с 2005 года пропало или было разглашено свыше 104 миллионов записей, содержащих частные сведения.)

Большинство организаций уже находятся под действием юридических или корпоративных документов, обязывающих охранять сведения личного характера, и даже если ваше предприятие еще не входит в их число, вы наверняка были бы заинтересованы обеспечить документам сохранность.

Зачем шифровать весь том?

Если вы опытный администратор Windows, вы наверняка уже знакомы с имевшимися в Windows вариантами шифрования, например EFS, и, возможно, с шифрованием и защитой служб управления правами (RMS). Главное отличие BitLocker в том, что он работает автоматически, прозрачно и распространяется на весь том.

Например, в EFS нужно было явно указывать, какие файлы и папки шифровать. В Windows Vista появились новые параметры, добавляющие EFS гибкости. И EFS, и RMS могут пригодиться в определенных обстоятельствах, когда BitLocker не сможет помочь. Обе эти технологии требуют значительных усилий по настройке и не предназначены для защиты всего содержимого тома.

В противоположность им, BitLocker шифрует все, что записывается на защищенный им том, включая файлы операционной системы, реестр, файлы спящего режима и подкачки, приложения и их данные.

Не шифруются три элемента: загрузочный сектор, поврежденные сектора, уже отмеченные как нечитаемые, и метаданные тома. Последние состоят из трех избыточных копий данных, используемых BitLocker, включая статистическую информацию о томе и защищенные копии некоторых ключей расшифровки. Эти элементы не требуют шифрования, поскольку не являются уникальными, ценными или позволяющими определить личность.

Шифрование всего тома защищает от атак с выключением (offline attack), которые подразумевают обход операционной системы. Типичный пример — кража офисного компьютера, извлечение жесткого диска и установка его в качестве второго диска другого компьютера (под управлением другой копии Windows или вообще другой ОС), что позволяет обойти разрешения NTFS и ввод пароля. Прочитать таким образом диск, защищенный BitLocker, невозможно.

Как BitLocker шифрует данные

BitLocker использует алгоритм AES с ключом 128 бит. Для большей надежности длину ключа можно увеличить до 256 бит с помощью групповых политик или через поставщик инструментария управления Windows (WMI) для BitLocker.

Каждый сектор тома шифруется отдельно, при этом часть ключа шифрования определяется номером этого сектора. В результате два сек-

тора, содержащие одинаковые незашифрованные данные, будут в зашифрованном виде выглядеть по-разному, что сильно затрудняет определение ключей шифрования путем записи и шифровки заранее известных данных.

Перед применением шифрования BitLocker использует алгоритм, называемый диффузором (diffuser). Не углубляясь в криптографию, можно сказать, в результате его применения даже мельчайшее изменение исходного текста приводит к абсолютному изменению всего сектора зашифрованных данных. Это также серьезно затрудняет определение ключей или дешифровку.

Если вас заинтересовали детали алгоритма шифрования BitLocker, вы можете подробнее прочитать о нем в статье Нейла Фергюсона (Neil Ferguson) «[AES-CBC + Elephant Diffuser: алгоритм шифрования диска для Windows Vista](#)».

Ключи BitLocker

Имея дело с шифрованием, стоит разбираться в ключах, и шифрование BitLocker не исключение. Архитектура его ключей изящна, но весьма непростая.

Сами секторы шифруются ключом шифрования всего тома (full-volume encryption key, FVEK). Пользователи, однако, с этим ключом не работают и доступа к нему не имеют. Сам ключ FVEK шифруется основным ключом тома (volume master key, VMK). Такой уровень абстракции дает уникальные преимущества, но делает весь процесс более трудным для понимания. Ключ FVEK хранится в строжайшей секретности, потому что при его разглашении потребовалось бы перешифровать все секторы. Поскольку перешифрование займет значительное время, стоит не допускать разглашения ключа. Поэтому система работает с ключом VMK.

Ключ FVEK (зашифрованный ключом VMK) хранится на диске среди метаданных тома. При этом он никогда не попадает на диск в расшифрованном виде.

Ключ VMK тоже шифруется, или «охраняется», одним или несколькими предохранителями ключей. Предохранитель по умолчанию — TPM. Его использование описано далее в разделе о проверке целостности. Пароль восстановления тоже создается как предохранитель на случай экстренных ситуаций. Восстановление также описано далее.

Для дополнительной защищенности можно объединить TPM с числовым ПИН-кодом или с частичным ключом, хранимым на USB-накопителе. И то, и другое — образец двухфакторной проверки подлинности. Если у компьютера нет совместимого TPM-чипа и BIOS, BitLocker может сохранить предохранитель ключа целиком на USB-накопителе. Получится ключ запуска.

BitLocker можно отключить, не расшифровывая данные. В этом случае ключ VMK защищается только новым предохранителем ключа, который хранится в незашифрованном виде. Этот ключ позволяет системе получать доступ к диску так, словно он не зашифрован.

При запуске система ищет подходящий предохранитель ключа, опрашивая TPM, проверяя порты USB или, если необходимо, запрашивая пользователя (что называется восстановлением). Обнаружение предохранителя ключа позволяет Windows расшифровать ключ VMK, которым расшифровывается ключ FVEK, которым расшифровываются данные на диске.

Весь процесс показан на рис. 1.

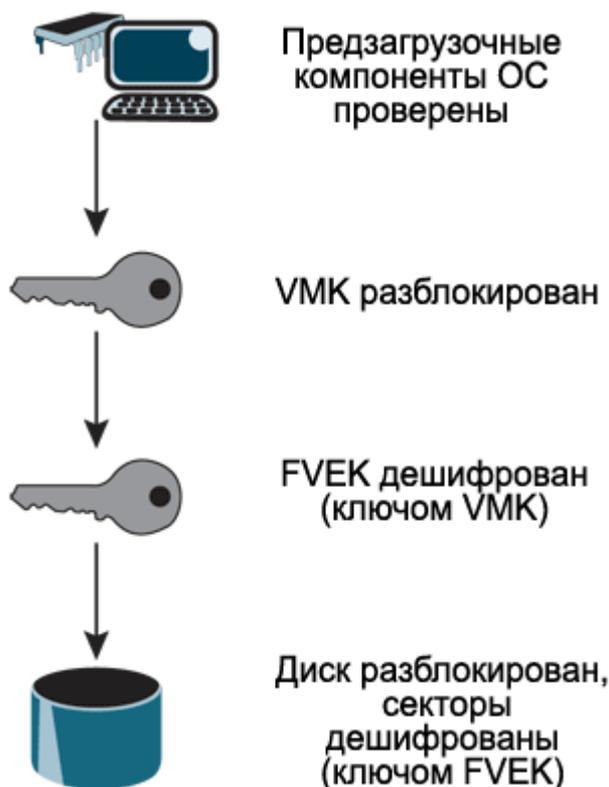


Рис. 1 Процесс запуска BitLocker по умолчанию

Проверка целостности

Поскольку компоненты, выполняющие начальную стадию загрузки, должны оставаться незашифрованными (иначе компьютер не сможет запуситься), злоумышленник может изменить их код (создать rootkit) и так получить доступ к компьютеру, даже если данные на диске останутся зашифрованными.

Это открывает доступ к конфиденциальной информации, например ключам BitLocker или паролям пользователей, которые могут быть использованы для обхода других средств защиты.

Предотвращение такого хода событий было одной из исходных целей всей программы и группы разработчиков BitLocker. До некоторой

степени, шифрование почти позволяло достичь конечной цели. Полное шифрование тома позволяет BitLocker сберегать целостность системы и не давать Windows загрузиться, если компоненты, выполняющие начальную стадию загрузки, были изменены.

Если компьютер снабжен совместимым TPM, при каждом его запуске каждый из компонентов ранней загрузки — BIOS, MBR, загрузочный сектор и код диспетчера загрузки — проверяет запускаемый код, подсчитывает значение хэша и сохраняет его в специальных регистрах TPM, называемых регистрами конфигурации платформы (platform configuration registers, PCR). Значение, сохраненное в PCR, может быть заменено или стерто только при перезапуске системы. BitLocker использует TPM и значения, сохраненные в PCR, для защиты ключа VMK.

TPM может создать ключ, привязанный к конкретным значениям PCR. После создания этот ключ шифруется модулем TPM, и расшифровать его сможет только этот конкретный модуль. Причем для этого потребуется, чтобы текущие значения PCR совпадали со значениями на момент создания ключа. Это называется запечатыванием (sealing) ключа в TPM.

По умолчанию BitLocker запечатывает ключи к измерениям CRTM, BIOS и любым расширениям платформы, необязательному ROM-коду, коду MBR, загрузочному сектору NTFS и диспетчеру загрузки. Если любой из этих элементов неожиданно оказывается измененным, BitLocker блокирует диск и не даст получить к нему доступ или расшифровать.

По умолчанию BitLocker настроен на обнаружение и использование TPM. С помощью настроек групповой или локальной политики можно разрешить работу BitLocker без TPM с хранением ключей на внешнем флэш-накопителе USB, но тогда становится невозможно проверять целостность системы.

Первичное включение BitLocker

BitLocker доступен в редакциях Windows Vista Enterprise и Windows Vista Ultimate (а также как необязательный компонент следующей версии Windows Server® под кодовым именем «Longhorn»).

В нижеследующем изложении предполагается, что для тестирования доступен компьютер с совместимым TPM. Если требуется включить BitLocker на компьютере без TPM, следуйте инструкциям на боковой панели «Использование BitLocker без TPM».

Использование BitLocker без TPM

По умолчанию BitLocker настроен на использование TPM, поэтому при его отсутствии Windows с неизменными настройками не даст включить BitLocker. Однако, выполнив приведенные далее шаги, взятые

из «Пошагового руководства шифрования дисков Windows BitLocker», вы сможете использовать BitLocker на компьютере без TPM.

Для выполнения этих шагов необходимо войти в систему с администраторскими привилегиями. Даже при отсутствии TPM компьютер должен поддерживать чтение с флэш-накопителя USB во время загрузки. Кроме того, необходимо иметь и сам готовый к использованию флэш-накопитель — при запуске BitLocker и при каждой последующей перезагрузке компьютера.

Шифрование диска BitLocker на компьютере без совместимого TPM включается так:

1. нажмите кнопку Пуск, введите `gpedit.msc` в поле поиска и нажмите ВВОД;
2. если появится диалоговое окно контроля учетных записей, подтвердите желаемость действия, нажав кнопку «Продолжить»;
3. в дереве консоли редактора объектов групповых политик выберите пункт «Редактор локальной политики», щелкните «Административные шаблоны», затем «Компоненты Windows», после чего дважды щелкните «Шифрование диска BitLocker»;
4. Дважды щелкните настройку «Установка панели управления: включить дополнительные параметры запуска». Появится одноименное диалоговое окно;
5. Выберите вариант «Включить», установите флажок «Разрешить использование BitLocker без совместимого TPM» и нажмите кнопку «ОК». Теперь вместо TPM можно использовать ключ запуска;
6. закройте редактор объектов групповой политики;
7. чтобы новые настройки групповых политик вступили в силу немедленно, нажмите кнопку «Пуск», введите `groupdate.exe /force` в поле поиска и нажмите клавишу ВВОД. Дождитесь завершения процесса.

Важный шаг в процессе включения BitLocker — убедиться, что тома настроены верно. Для работы BitLocker требуется, чтобы активный раздел был не зашифрован. Это необходимо для считывания загрузочного сектора, диспетчера загрузки и загрузчика Windows (эти компоненты защищаются средствами проверки целостности системы, описанными ранее). Поскольку другие компоненты Windows могут нуждаться во временном доступе к активному разделу, корпорация Майкрософт рекомендует отводить ему не меньше 1,5 ГБ. Также не помешает настроить разрешения NTFS, чтобы пользователи не смогли случайно записать данные на этот том.

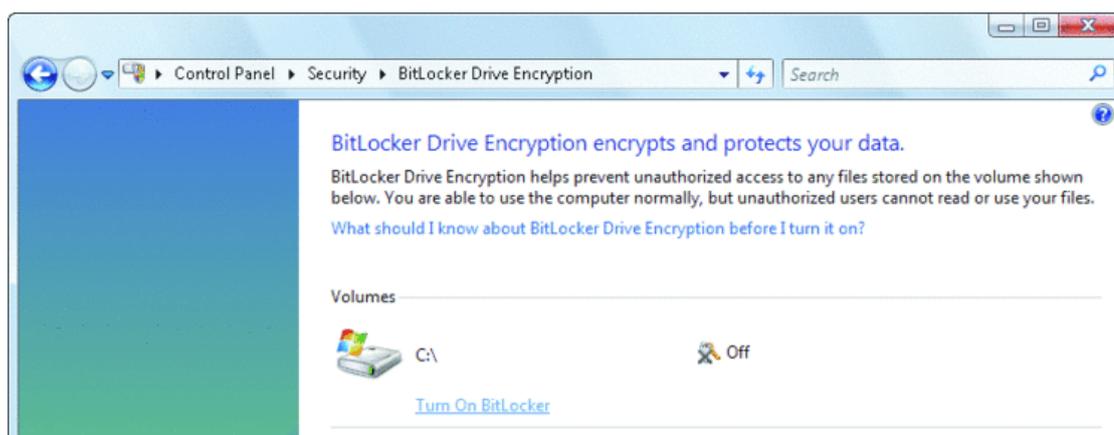
Сама Windows будет установлена на другой, больший том, который можно зашифровать. Если установка Windows производится на новый компьютер, можно вручную настроить тома в соответствии с инструк-

циями, приведенными в [Пошаговом руководстве шифрования дисков Windows BitLocker](#).

Для подготовки системы можно использовать средство подготовки диска для BitLocker. Это средство берет на себя все заботы по настройке дисков. Оно доступно как Windows Vista Ultimate Extra, а также для потребителей, занимающихся развертыванием Windows Vista Enterprise. Подробные инструкции по использованию этого средства см. в статье базы знаний support.microsoft.com/kb/930063.

Средство подготовки автоматически уменьшает размер тома (если он один), создает второй раздел, делает его активным, вносит все необходимые изменения в конфигурацию и переносит стартовые файлы в нужное место.

После настройки томов включить BitLocker не составляет труда. В разделе «Безопасность» панели управления щелкните значок шифрования дисков BitLocker. После утвердительного ответа на запрос UAC появится диалоговое окно, показанное на рис. 2.



Дальнейшая последовательность шагов зависит от состояния микросхемы TPM компьютера. Если он не инициализирован, запустится мастер инициализации TPM. Для успешной инициализации следуйте его указаниям (потребуется перезагрузить компьютер).

После инициализации TPM появится страница сохранения пароля восстановления (рис. 3). Пароль восстановления нужен для возвращения доступа к данным в случае сбоя в модуле TPM или другой неисправности. С помощью этой страницы можно сохранить его на флэш-накопителе USB или на сетевом диске, а также напечатать для помещения в безопасное место. Нужно выбрать хотя бы один из этих вариантов, причем сохранять можно в нескольких экземплярах. После сохранения кнопка «Далее» станет доступной. Нажмите ее.

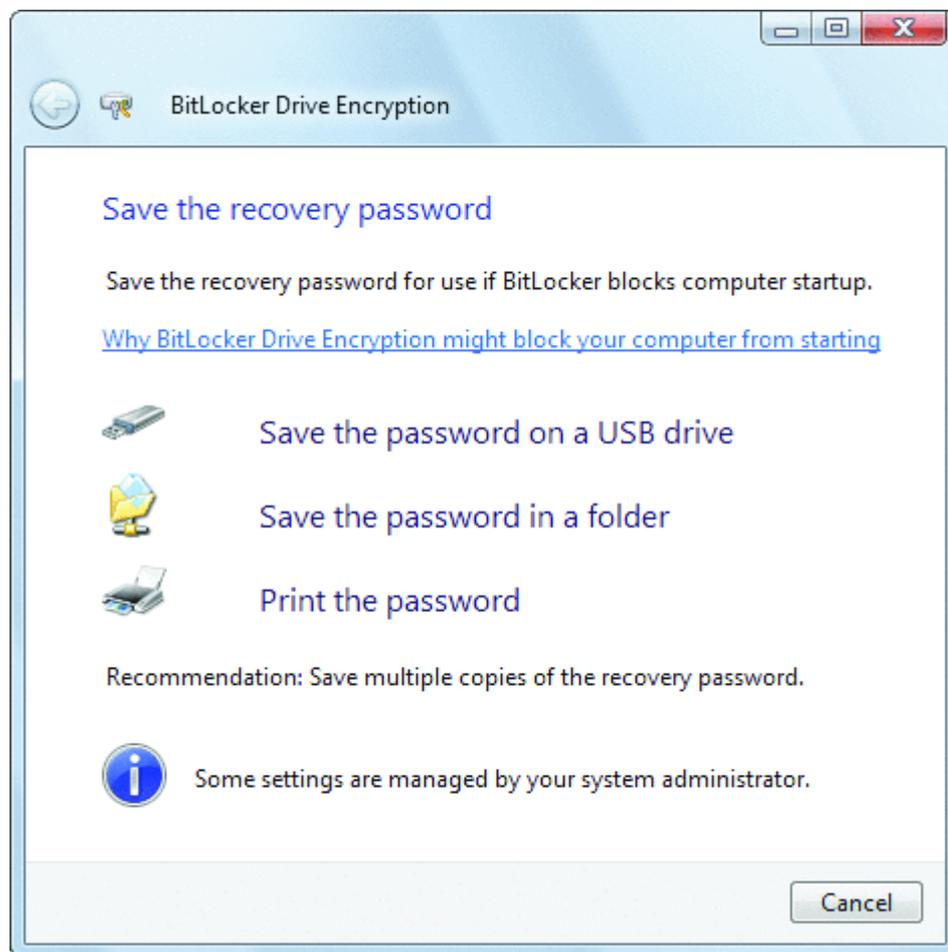


Рис. 3 Сохранение пароля восстановления

На следующей странице — «Зашифровать выбранный том» — можно указать, запускать ли проверку системы перед шифрованием. Проверка потребует перезагрузки, но это лучший способ убедиться, что TPM, BIOS и порты USB будут успешно использованы BitLocker. Если возникли проблемы, после перезагрузки будет отображено сообщение об ошибке. В противном случае появится строка состояния «Выполняется шифрование».

Вот и все Шифрование продолжит выполняться в фоновом режиме, а вы можете продолжать использовать свой компьютер. После завершения шифрования появляется соответствующее сообщение. Можно самостоятельно отслеживать текущее состояние шифрования, перемещая курсор на значок шифрования диска BitLocker в панели инструментов внизу экрана. Подробнее весь процесс описан в пошаговом руководстве, упомянутом выше.

Некоторых пользователей удивляет, что при запуске компьютера BitLocker не запрашивает ничего у пользователя и не вмешивается каким-либо иным заметным способом. Это происходит потому, что по умолчанию в проверке целостности системы до разблокировки диска BitLocker полагается на TPM. Это происходит автоматически и прозрачно для пользователя.



Рис. 5 Ввод пароля BitLocker

Теперь BitLocker ожидает ввода 48-значного цифрового пароля, который разблокирует диск. Это число напечатано на странице, если была выбрана печать пароля восстановления, или хранится в файле, если был выбран этот вариант сохранения.

Простейший путь управления паролями восстановления в рамках предприятия — их автоматическое хранение в службах Active Directory®. Подробно об этом см. go.microsoft.com/fwlink/?LinkId=87067.

В следующей статье мы подробно остановимся на управляемости BitLocker, а пока достаточно сказать, что он поставляется с полноценным поставщиком WMI, который позволяет контролировать BitLocker (и TPM) через любую совместимую с WMI систему WBEM. Это, в частности, означает, что управлять BitLocker можно через сценарии на любом языке сценариев, способном получать доступ к объектам WMI, например VBScript и Windows PowerShell™.

Вместе с BitLocker также поставляется средство командной строки `manage-bde.wsf`, использующее провайдер WMI для управления BitLocker на локальном и удаленном компьютере. Для получения более подробной информации о нем запустите командную строку с повышенными привилегиями и введите `manage-bde.wsf /?`.

Безопасное списание

Каждый компьютер в конце концов приходится списывать. Обычно предприятия тратят значительные средства и усилия на то, чтобы диски таких компьютеров были предварительно полностью очищены. Большинство методов удаления секретных данных требуют значительного времени и денег или выливаются в полное уничтожение оборудования. Средство BitLocker предоставляет более эффективные решения.

Вместо фактического удаления данных BitLocker гарантирует, что секретные сведения не хранятся на диске небезопасным образом. Поскольку все содержимое диска зашифровано, данные можно считать навсегда утерянными, если уничтожены все копии ключей шифрования. Сам жесткий диск остается неповрежденным и может быть повторно использован.

Существует большое число подходов к списанию томов, защищенных BitLocker. Можно удалить все копии ключей из метаданных тома, оставив их копии в надежно защищенном центральном архиве. После этого можно без опаски перевозить компьютеры или временно списать, если им предстоит провести значительное время без работы. Это гарантирует, что авторизованные пользователи смогут получить доступ к данным, в то время как все остальные, например новые владельцы оборудования, — нет.

Можно удалить все копии ключей из метаданных тома и из всех архивов, таких как Active Directory (это можно сделать, например, созданием новых ключей, которые нигде не будут храниться). Без ключей расшифровки никто не сможет восстановить данные.

В любом из этих случаев удаление и уничтожение ключей, содержащихся в метаданных тома, производится практически мгновенно и может выполняться администратором на многих системах разом. На это требуется минимум сил и времени, а результат — очень высокая степень непрерывной защиты. Средство форматирования в Windows Vista было обновлено. Теперь команда `format` удаляет метаданные тома и перезаписывает их секторы для надежного удаления всех ключей BitLocker.

Несколько заключительных слов

BitLocker — мощное средство, разработанное для защиты от конкретных угроз, с чем оно прекрасно справляется. Но не стоит считать его панацеей. Совершенно необходимо продолжать использование остальных защитных и управляющих мер, например надежных паролей.

BitLocker предназначен для защиты от атак с отключением оборудования. Если Windows запущена, BitLocker разблокировал том. Иными словами, он не обеспечивает защиту работающей системы. В этом его дополняют такие технологии, как EFS и RMS.

Подробнее о BitLocker см. на веб-узле Майкрософт, начиная с technet.microsoft.com/windowsvista/aa905065.aspx. Подробнее о спецификациях TPM и TCG см. в разделе «TPM Specifications» веб-узла TCG по адресу go.microsoft.com/fwlink/?LinkId=72757.

По материалам сайта:

<http://www.securitylab.ru/analytics/296866.php>